

# ON THE ODLYZKO-STANLEY ENUMERATION PROBLEM AND WARING'S PROBLEM OVER FINITE FIELDS

JIYOU LI

ABSTRACT. We obtain an asymptotic formula on the Odlyzko-Stanley enumeration problem. Let  $N_m^*(k, b)$  be the number of  $k$ -subsets  $S \subseteq \mathbf{F}_p^*$  such that  $\sum_{x \in S} x^m = b$ . If  $m < p^{1-\delta}$ , then there is a constant  $\epsilon = \epsilon(\delta) > 0$  such that

$$\left| N_m^*(k, b) - p^{-1} \binom{p-1}{k} \right| \leq \binom{p^{1-\epsilon} + mk - m}{k}.$$

In addition, let  $\gamma'(m, p)$  denote the distinct Waring's number (mod  $p$ ), the smallest positive integer  $k$  such that every integer is a sum of  $m$ -th powers of  $k$ -distinct elements (mod  $p$ ). The above bound implies that there is a constant  $\epsilon(\delta) > 0$  such for any prime  $p$  and any  $m < p^{1-\delta}$ , if  $\epsilon^{-1} < (e-1)p^{\delta-\epsilon}$ , then

$$\gamma'(m, p) \leq \epsilon^{-1}.$$

## 1. INTRODUCTION

Let  $p$  be an odd prime, and let  $\mathbf{F}_p$  be the prime field of order  $p$ . Let  $m$  be a positive integer and  $b$  be an element in  $\mathbf{F}_p$ . Let  $N_m^*(b)$  be the number of subsets  $S \subseteq \mathbf{F}_p^*$  with the property that

$$\sum_{x \in S} x^m = b.$$

If  $S$  is the empty set, we set  $\sum_{x \in \emptyset} x^m = 0$ . For details of this problem we refer to [23]. It was shown by Odlyzko-Stanley [22] that

$$|N_m^*(b) - 2^{p-1}p^{-1}| \leq e^{O(m\sqrt{p}\log p)}. \quad (1.1)$$

This bound can be improved to a sharper bound

$$|N_m^*(b) - 2^{p-1}p^{-1}| \leq \frac{4}{\sqrt{2\pi}} e^{m\sqrt{p}\log p}. \quad (1.2)$$

Moreover, if  $\mathbf{F}_p^*$  is replaced by  $\mathbf{F}_q^*$ , the multiplication group of a finite field of order  $q$  and of characteristic  $p$ , then

$$|N_m^*(b) - 2^{q-1}q^{-1}| \leq \frac{4p}{\sqrt{2\pi}q} e^{(m\sqrt{q}+q/p)\log q}. \quad (1.3)$$

These bounds follow directly from several counting formulas obtained by Zhu-Wan [25]. Their proof combines the techniques of Gauss sums, Jacobi sums and a new sieving argument. More precisely, let  $N_m^*(k, b)$  be the number of  $k$ -subsets  $S \subseteq \mathbf{F}_q^*$  such that  $\sum_{x \in S} x^m = b$ . They proved that

$$\left| N_m^*(k, b) - q^{-1} \binom{q-1}{k} \right| \leq 2q^{-1/2} \binom{m\sqrt{q} + q/p + k}{k}. \quad (1.4)$$

---

This work is supported by the National Science Foundation of China (11001170).

Note that  $N_m^*(b) = \sum_{k=0}^q N_m^*(k, b)$  and it is sufficient to consider the case  $|S| \leq (q-1)/2$  by symmetry. Hence (1.2) and (1.3) follow from (1.4) directly.

Note that all above bounds are nontrivial only when  $n < p^{1/2-\epsilon}$ . Heath-Brown, Konyagin and Shparlinski [16, 19] improved this restriction to  $n < p^{\frac{2}{3}-\epsilon}$ . Precisely, they obtain

$$|N_m^*(b) - 2^{p-1}p^{-1}| \leq \begin{cases} e^{O(mp^{1/2} \log p)}, & m \leq p^{1/3}; \\ e^{O(m^{5/8}p^{5/8} \log p)}, & p^{1/3} \leq m \leq p^{1/2}; \\ e^{O(m^{3/8}p^{3/4} \log p)}, & p^{1/2} \leq m \leq p^{2/3}. \end{cases}$$

Their proof relies on the monomial exponential sum bound

$$\left| \sum_{x \in \mathbf{F}_p^*} e_p(ax^m) \right| \ll \begin{cases} mp^{1/2}, & m \leq p^{1/3}; \\ m^{5/8}p^{5/8}, & p^{1/3} \leq m \leq p^{1/2}; \\ m^{3/8}p^{3/4}, & p^{1/2} \leq m \leq p^{2/3}; \end{cases}$$

for any integer  $a$  with  $p \nmid a$ , where  $e_p(x) = e^{2\pi i x/p}$  is the additive character on  $\mathbf{F}_p$ . Cochrane and Pinner [10] made explicit this bound to that

$$\left| \sum_{x \in \mathbf{F}_p^*} e_p(ax^m) \right| \leq \begin{cases} mp^{1/2}, & m \leq 3p^{1/3}; \\ \lambda m^{5/8}p^{5/8}, & 3p^{1/3} \leq m < p^{1/2}; \\ \lambda m^{3/8}p^{3/4}, & p^{1/2} \leq m < \frac{1}{3}p^{2/3}; \end{cases}$$

where  $\lambda$  can be chosen to be  $2/\sqrt[3]{4} \approx 1.51967$ .

When  $m$  is large, Bourgain and Konyagin [2, 4, 5] obtained a celebrated nontrivial bound for a large kind of subgroups. Let  $H$  be a subgroup of  $\mathbf{F}_p^*$ . Suppose  $|H| > p^\delta$ , then there exists a constant  $\delta' > 0$  such that for any integer  $a$  with  $p \nmid a$ ,

$$\left| \sum_{x \in H} e_p(ax) \right| < |H|^{1-\delta'}. \quad (1.5)$$

For instance, Bourgain and Garaev proved in [3] that if  $\delta > 1/4$ , then one can take  $\delta' = 0.000015927 + o(1)$ . Taking  $H = \{x^m, x \in \mathbf{F}_p^*\}$  and following the same argument of Konyagin and Shparlinski [19], the above bound immediately implies that if  $m < p^{1-\delta}$ , then

$$N_m^*(b) = 2^{p-1}p^{-1} + e^{O(p^{1-\epsilon})}, \quad (1.6)$$

where  $\epsilon = \epsilon(\delta)$  is a positive constant. This is a significant improvement of (1.1).

In this paper, by using the above bound and a distinct coordinate sieve argument, we first consider the subset sum problem over  $H \subseteq \mathbf{F}_p^*$  and thus obtain a new counting formula via a combinatorial argument. It gives a more precise bound on the number  $N_m^*(k, b)$  for  $m < p^{1-\delta}$  and suitable  $k$ . It is proved in this paper that

**Theorem 1.1.** *Let  $N_m^*(k, b)$  be the number of  $k$ -subsets  $S \subseteq \mathbf{F}_p^*$  such that  $\sum_{x \in S} x^m = b$ . If  $m < p^{1-\delta}$ , then there is a constant  $0 < \epsilon = \epsilon(\delta) < \delta$  such that*

$$\left| N_m^*(k, b) - p^{-1} \binom{p-1}{k} \right| \leq \binom{p^{1-\epsilon} + mk - m}{k}. \quad (1.7)$$

**Corollary 1.2.** *Suppose that  $p, m, s, \delta, \epsilon$  are as in Theorem 1.1. If there is a constant  $0 < c < 1$  such that  $-\frac{1}{\log c} \log p < k < cp^\delta - p^{\delta-\epsilon}$ , then the equation*

$$x_1^m + x_2^m + \cdots + x_k^m = b, \quad x_i \in \mathbf{F}_p^*, \quad x_i \neq x_j, \quad i \neq j$$

has at least a solution. In particular, if  $\epsilon^{-1} < k < (e-1)p^{\delta-\epsilon}$ , then the above equation has a solution.

Note that this is a constant lower bound. This corollary has direct application to the subset version of Waring's number mod  $p$ . We first recall the definition of ordinary Waring's number. Let  $\gamma(m, p)$  denote Waring's number (mod  $p$ ), the smallest positive integer  $k$  such that every integer is a sum of  $m$ -th power (mod  $p$ ). This number has been thoroughly studied. Note that we can always assume that  $m < (p-1)/2$ . The first bound

$$\gamma(m, p) \leq m$$

for any prime  $p$  was proved by Cauchy in 1813, as reported in [1]. Dozens of papers, for instance, [11, 12, 13, 14, 15, 17, 18, 6, 24], studied Waring's number mod a prime number, and generally, Waring's number mod an integer, Waring's number over finite fields,  $p$ -adic integers and a general commutative ring. We refer to [7] for the previous results of this problem.

The recent progress obtained by Ciper, Cocharane and Pinner [7] states that for any  $\epsilon > 0$  there is a constant  $c(\epsilon)$  such that if  $\phi(s) \geq 1/\epsilon$  then

$$\gamma(m, p) \leq c(\epsilon)m^\epsilon,$$

where  $s = (p-1)/m$  and  $\phi$  is the Euler's totient function. By the bound of Bourgain and Konyagin, and by a similar argument of Konyagin and Shparlinski [19], one can easily get

**Corollary 1.3.** *There is an absolute constant  $C > 0$  such that for  $m < p^{1-\delta}$ ,*

$$\gamma(m, p) \leq C^{1/\delta}.$$

Cochrane and Cipra [8] showed that  $C$  can be chosen to be 4 and  $\gamma(m, p) \ll 4^{1/\delta}$ .

We now consider a stronger version of Waring's number, namely, the distinct or subset version of Waring's number. Let  $\gamma'(m, p)$  denote the distinct Waring's number (mod  $p$ ), the smallest positive integer  $k$  such that every integer is a sum of  $m$ -th power of  $k$  distinct elements (mod  $p$ ). Note that there are big differences between the two Waring's numbers  $\gamma(m, p)$  and  $\gamma'(m, p)$ . For example,  $\gamma'(m, p)$  does not exist  $k$  is too large.

**Corollary 1.4.** *There is a constant  $\epsilon(\delta) > 0$  such that for any prime  $p$  and any  $m < p^{1-\delta}$ , if  $\epsilon^{-1} < (e-1)p^{\delta-\epsilon}$ , then we have*

$$\gamma'(m, p) < \epsilon^{-1}.$$

Obviously  $\gamma(m, p) \leq \gamma'(m, p)$  and thus this bound implies Corollary 1.3, the known constant bound for ordinary Waring's number.

Now we turn to the case for finite fields. Let  $\mathbf{F}_q$  be the finite field of order  $q$  and of characteristic  $p$ . Let  $\gamma(m, q)$  denote the Waring's number in  $\mathbf{F}_q$ , the smallest positive integer  $k$  such that every element in  $\mathbf{F}_q^*$  is a sum of  $m$ -th power in  $\mathbf{F}_q$ . The work of A. Winterhof [24] shows that

$$\gamma(m, q) \ll \frac{\log q}{\log p} m^{\log p / \log q} \log m$$

and J. Cipra [6] improved this bound to

$$\gamma(m, q) \ll \frac{\log q}{\log p} m^{\log p / \log q}.$$

Recently, Cochrane and Cipra [8] proved that

$$\gamma(m, q) \leq 633(2m)^{\frac{\log 4}{\log p - \log m}},$$

provided  $m < p$  and  $\gamma(m, q)$  exists.

Similarly let  $\gamma'(m, q)$  denote the distinct Waring's number over  $\mathbf{F}_q$ , the smallest positive integer  $k$  such that every element in  $\mathbf{F}_q$  is a sum of  $m$ -th power of distinct elements in  $\mathbf{F}_q^*$ . Clearly  $\gamma(m, q) \leq \gamma'(m, q)$ . The bound (1.4) given by Zhu-Wan can improve the above bound for Waring's number over finite fields. Using (1.4), Zhu and Wan obtained:

**Corollary 1.5.** [25] *There is an effectively computable absolute constant  $0 < c < 1$  such that if  $m < c\sqrt{q}$  and  $6 \ln q < k < (q-1)/2$  then  $N_m^*(k, b) > 0$  for all  $b \in \mathbf{F}_q$ .*

This certainly implies a sharper bound at some cases:

**Corollary 1.6.** *There is a constant  $c > 0$  such that if  $m < c\sqrt{q}$*

$$\gamma(m, q) \leq \gamma'(m, q) < \lfloor 6 \ln q \rfloor + 1.$$

This paper is organized as follows. Proof of the main result will be given in Section 3 and a distinct coordinate sieving method will be introduced briefly in Section 2.

**Notations.** For  $x \in \mathbb{R}$ , let  $(x)_0 = 1$  and  $(x)_k = x(x-1) \cdots (x-k+1)$  for  $k \in \mathbb{Z}^+$ . For  $k \in \mathbb{N}$ ,  $\binom{x}{k}$  is the binomial coefficient defined by  $\binom{x}{k} = \frac{(x)_k}{k!}$ .

## 2. A DISTINCT COORDINATE SIEVING FORMULA

In this section we introduce a sieving formula discovered by Li-Wan [20], which significantly improves the classical inclusion-exclusion sieve in many interesting cases. We cite it here without any proof. For details and related applications please refer to [20, 21].

Let  $D$  be a finite set, and let  $D^k$  be the Cartesian product of  $k$  copies of  $D$ . Let  $X$  be a subset of  $D^k$ . Define  $\overline{X} = \{(x_1, x_2, \dots, x_k) \in X \mid x_i \neq x_j, \forall i \neq j\}$ . Let  $f(x_1, x_2, \dots, x_k)$  be a complex valued function defined over  $X$  and

$$F = \sum_{x \in \overline{X}} f(x_1, x_2, \dots, x_k).$$

Let  $S_k$  be the symmetric group on  $\{1, 2, \dots, k\}$ . Each permutation  $\tau \in S_k$  factorizes uniquely as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. Two permutations in  $S_k$  are conjugate if and only if they have the same type of cycle structure (up to the order). For  $\tau \in S_k$ , define the sign of  $\tau$  to  $\text{sign}(\tau) = (-1)^{k-l(\tau)}$ , where  $l(\tau)$  is the number of cycles of  $\tau$  including the trivial cycles. For a permutation  $\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$  with  $1 \leq a_i, 1 \leq i \leq s$ , define

$$X_\tau = \{(x_1, \dots, x_k) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \dots, x_{l_1} = \cdots = x_{l_{a_s}}\}. \quad (2.1)$$

Similarly, for  $\tau \in S_k$ , define  $F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \dots, x_k)$ . Now we can state our sieve formula. We remark that there are many other interesting corollaries of this formula. For interested reader we refer to [20].

**Theorem 2.1.** *Let  $F$  and  $F_\tau$  be defined as above. Then*

$$F = \sum_{\tau \in S_k} \text{sign}(\tau) F_\tau. \quad (2.2)$$

Note that the symmetric group  $S_k$  acts on  $D^k$  naturally by permuting coordinates. That is, for  $\tau \in S_k$  and  $x = (x_1, x_2, \dots, x_k) \in D^k$ ,  $\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(k)})$ . A subset  $X$  in  $D^k$  is said to be symmetric if for any  $x \in X$  and any  $\tau \in S_k$ ,  $\tau \circ x \in X$ . For  $\tau \in S_k$ , denote by  $\bar{\tau}$  the conjugacy class determined by  $\tau$  and it can also be viewed as the set of permutations conjugate to  $\tau$ . Conversely, for given conjugacy class  $\bar{\tau} \in C_k$ , denote by  $\tau$  a representative permutation of this class. For convenience we usually identify these two symbols.

In particular, if  $X$  is symmetric and  $f$  is a symmetric function under the action of  $S_k$ , we then have the following simpler formula than (2.2).

**Corollary 2.2.** *Let  $C_k$  be the set of conjugacy classes of  $S_k$ . If  $X$  is symmetric and  $f$  is symmetric, then*

$$F = \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_{\tau}, \quad (2.3)$$

where  $C(\tau)$  is the number of permutations conjugate to  $\tau$ .

For the purpose of our proof, we will also need a combinatorial formula. A permutation  $\tau \in S_k$  is said to be of type  $(c_1, c_2, \dots, c_k)$  if  $\tau$  has exactly  $c_i$  cycles of length  $i$ . Note that  $\sum_{i=1}^k i c_i = k$ . Let  $N(c_1, c_2, \dots, c_k)$  be the number of permutations in  $S_k$  of type  $(c_1, c_2, \dots, c_k)$  and it is well-known that

$$N(c_1, c_2, \dots, c_k) = \frac{k!}{1^{c_1} c_1! 2^{c_2} c_2! \dots k^{c_k} c_k!}.$$

**Lemma 2.3.** *Define the generating function*

$$C_k(t_1, t_2, \dots, t_k) = \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) t_1^{c_1} t_2^{c_2} \dots t_k^{c_k}.$$

If  $t_1 = t_2 = \dots = t_k = q$ , then we have

$$\begin{aligned} C_k(q, q, \dots, q) &= \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) q^{c_1} q^{c_2} \dots q^{c_k} \\ &= (q + k - 1)_k. \end{aligned} \quad (2.4)$$

### 3. PROOF OF THEOREM 1.1

Let  $D \subseteq \mathbf{F}_p^*$  be a nonempty subset of cardinality  $n$ . Let  $\chi_a = e_p(ax) = e^{2\pi i ax/p}$  be an additive character over  $\mathbf{F}_p$  and  $\chi_0$  be the principal character sending each element in  $\mathbf{F}_p$  to 1. Denote by  $\widehat{\mathbf{F}}_p$  is the group of additive characters of  $\mathbf{F}_p$ . Define  $\Phi(D) = \max_{\chi \in \widehat{\mathbf{F}}_p, \chi \neq \chi_0} |\sum_{a \in D} \chi(a)|$ . Let  $N(k, b, D)$  be the number of  $k$ -subsets  $S \subseteq D$  such that  $\sum_{x \in S} x = b$ . In the following lemma we will give an asymptotic bound on  $N(k, b, D)$  when  $\Phi(D)$  is small compared to  $n = |D|$ .

**Lemma 3.1.** *Let  $N(k, b, D)$  be defined as above. Then*

$$\left| N(k, b, D) - p^{-1} \binom{n}{k} \right| \leq \binom{\Phi(D) + k - 1}{k}.$$

*Proof.* Let  $X = D^k = D \times D \times \dots \times D$  be the Cartesian product of  $k$  copies of  $D$ . Let  $\overline{X} = \{(x_1, x_2, \dots, x_k) \in D^k \mid x_i \neq x_j, \forall i \neq j\}$ . It is clear that  $|X| = n^k$  and  $|\overline{X}| = (n)_k$ . Then

$$\begin{aligned}
k!N(k, b, D) &= p^{-1} \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \sum_{\chi \in \widehat{\mathbf{F}}_p} \chi(x_1 + x_2 + \dots + x_k - b) \\
&= p^{-1}(n)_k + p^{-1} \sum_{\chi \neq \chi_0} \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \chi(x_1)\chi(x_2) \cdots \chi(x_k)\chi^{-1}(b) \\
&= p^{-1}(n)_k + p^{-1} \sum_{\chi \neq \chi_0} \chi^{-1}(b) \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \prod_{i=1}^k \chi(x_i).
\end{aligned}$$

For  $\chi \neq \chi_0$ , let  $f_\chi(x) = f_\chi(x_1, x_2, \dots, x_k) = \prod_{i=1}^k \chi(x_i)$ , and for  $\tau \in S_k$  let

$$F_\tau(\chi) = \sum_{x \in X_\tau} f_\chi(x) = \sum_{x \in X_\tau} \prod_{i=1}^k \chi(x_i),$$

where  $X_\tau$  is defined as in (2.1). Obviously  $X$  is symmetric and  $f_\chi(x_1, x_2, \dots, x_k)$  is normal on  $X$ . Applying (2.3) in Corollary 2.2,

$$k!N(k, b, D) = p^{-1}(n)_k + p^{-1} \sum_{\chi \neq \chi_0} \chi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\chi),$$

where  $C_k$  is the set of conjugacy classes of  $S_k$ ,  $C(\tau)$  is the number of permutations conjugate to  $\tau$ , and

$$\begin{aligned}
F_\tau(\chi) &= \sum_{x \in X_\tau} \prod_{i=1}^k \chi(x_i) \\
&= \sum_{x \in X_\tau} \prod_{i=1}^{c_1} \chi(x_i) \prod_{i=1}^{c_2} \chi^2(x_{c_1+2i}) \cdots \prod_{i=1}^{c_k} \chi^k(x_{c_1+c_2+\dots+k i}) \\
&= \prod_{i=1}^k \left( \sum_{a \in D} \chi^i(a) \right)^{c_i}.
\end{aligned}$$

By the definition of  $\Phi(D)$ ,  $F_\tau(\chi) \leq (\Phi(D))^{\sum_{i=1}^k c_i}$  and hence

$$\begin{aligned}
k!N(k, b, D) &\geq p^{-1}(n)_k - p^{-1} \sum_{\chi \neq \chi_0} \sum_{\tau \in C_k} C(\tau) (\Phi(D))^{\sum_{i=1}^k c_i} \\
&= p^{-1}(n)_k - p^{-1}(p-1) \sum_{\sum i c_i = k} \frac{k!}{1^{c_1} c_1! 2^{c_2} c_2! \cdots k^{c_k} c_k!} (\Phi(D))^{\sum_{i=1}^k c_i} \\
&= p^{-1}(n)_k - (\Phi(D) + k - 1)_k. \quad \square
\end{aligned}$$

The last equality is from Lemma 2.3 and the proof is complete.

This lemma together with the bound (1.5) given by Bourgain and Konyagin gives the following lemma.

**Lemma 3.2.** *Choose  $H = \{x^m, x \in \mathbf{F}_p^*\}$ . Suppose that  $|H| = s > p^\delta$ . Let  $M(k, b) = M(k, b, H)$  be the number of  $k$ -subsets  $S \subseteq H$  such that  $\sum_{x \in S} x = b$ . Then we have*

$$\left| M(k, b) - p^{-1} \binom{s}{k} \right| \leq \binom{s^{1-\delta'} + k - 1}{k}.$$

Next lemma is a counting formula, which allows us to "lift" the solution of the subset sum problem in the subgroup to the Odlyzko-Stanley enumeration problem.

**Lemma 3.3.** *Suppose  $n \mid p-1$  and denote  $s = (p-1)/n$ . Then*

$$\begin{aligned} \binom{p-1}{k} &= \binom{s}{k} \binom{n}{1}^k + \binom{s}{k-1} (k-1) \binom{n}{1}^{k-2} \binom{n}{2} + \cdots \\ &+ \binom{s}{j} \sum_{i_1 > 0, i_2 > 0, \dots, i_j > 0, \sum_{t=1}^j i_t = k} \binom{n}{i_1} \binom{n}{i_2} \cdots \binom{n}{i_j} + \cdots + \binom{s}{1} \binom{n}{k}. \end{aligned}$$

*Proof.* It is direct by a double counting argument. The left side counts the number of  $k$ -subsets of  $p-1$  balls. Divide  $p-1$  balls into  $s$  equal boxes with each of size  $n$  and count the same number by two steps. Choose boxes first and then choose the balls in the chosen boxes. The number is exactly the right side.  $\square$

**Proof of Theorem 1.1** Choose  $H = \{x^m, x \in \mathbf{F}_p^*\}$ . We suppose that  $m \mid p-1$  without loss of generality, otherwise we can replace  $m$  by  $(m, p-1)$ . Note that  $|H| = s = (p-1)/m > p^\delta$ . Let  $M(k, b) = M(k, b, H)$  be the number of unordered solutions of the equation

$$x_1 + x_2 + \cdots + x_k = b, \quad x_i \in H, \quad x_i \neq x_j, \quad i \neq j. \quad (3.1)$$

By Lemma 3.2 we have

$$\left| M(k, b) - p^{-1} \binom{s}{k} \right| \leq \binom{s^{1-\delta'} + k - 1}{k}.$$

Recall  $N_m^*(k, b)$  is also the number of unordered solutions of the diagonal equation

$$x_1^m + x_2^m + \cdots + x_k^m = b, \quad x_i \in \mathbf{F}_p^*, \quad x_i \neq x_j, \quad i \neq j. \quad (3.2)$$

Similar to the proof of Lemma 3.3, any solution of (3.1) can be lifted to solutions of (3.2). This counting argument between (3.1) and (3.2) gives

$$\begin{aligned} N_m^*(k, b) &= M(k, b) \binom{m}{1}^k + M(k-1, b) (k-1) \binom{m}{1}^{k-2} \binom{m}{2} + \cdots \\ &+ M(j, b) \sum_{i_1 > 0, i_2 > 0, \dots, i_j > 0, \sum_{t=1}^j i_t = k} \binom{m}{i_1} \binom{m}{i_2} \cdots \binom{m}{i_j} + \cdots + M(1, b) \binom{m}{k}. \end{aligned}$$

By Lemma 3.3 this implies

$$\begin{aligned} \left| N_m^*(k, b) - p^{-1} \binom{p-1}{k} \right| &\leq \binom{ps^{-\delta'} + mk - m}{k} \\ &\leq \binom{p^{1-\epsilon} + mk - m}{k}, \end{aligned}$$

where  $\epsilon = \delta\delta'$  and the proof is complete.  $\square$

**Corollary 3.4.** *Suppose that  $p, m, s, \delta, \epsilon$  are as in Theorem 1.1. If there is a constant  $0 < c < 1$  such that  $-\frac{1}{\log c} \log p < k < cp^\delta - p^{\delta-\epsilon}$ , then the equation*

$$x_1^m + x_2^m + \cdots + x_k^m = b, \quad x_i \in \mathbf{F}_p^*, \quad x_i \neq x_j, \quad i \neq j.$$

*has at least a solution. In particular, if we choose  $c = ep^{-\epsilon}$ , we then have a simpler condition  $\epsilon^{-1} < k < (e-1)p^{\delta-\epsilon}$ , which has a constant lower bound.*

*Proof.* By Theorem 1.1, to ensure  $N_m^*(k, b) > 0$  it is sufficient to have

$$p^{-1} \binom{p-1}{k} \geq \binom{p^{1-\epsilon} + mk - m}{k},$$

that is,

$$\frac{(p-1)_k}{(p^{1-\epsilon} + mk - m)_k} > p.$$

This leads to the following inequality

$$\frac{p}{p^{1-\epsilon} + mk} > p^{1/k}.$$

Take  $0 < c < 1$  such that  $p^{1-\epsilon} + mk < p^{1-\epsilon} + p^{1-\delta}k < cp$  and we have  $c^{-1} > p^{1/k}$  and then  $k > -\frac{1}{\log c} \log p$ . Solve the first inequality we get that  $k < cp^\delta - p^{\delta-\epsilon}$ . If  $c = ep^{-\epsilon}$ , then the condition becomes  $k > \frac{\log p}{\epsilon \log p - 1} > \epsilon^{-1}$ .  $\square$

**Open Question 3.5.** *Is it true that the bound*

$$\left| N_m^*(k, b) - p^{-1} \binom{p-1}{k} \right| \leq \binom{p^{1-\epsilon} + k - 1}{k}$$

*holds as (1.4) for any  $m < p^{1-\delta}$ ?*

If this bound is true, then the bound (1.6) will be strengthened by a significantly large error term and the bound in Corollary 3.4 will be improved.

#### REFERENCES

- [1] A. Alnaser and T. Cochrane, *Waring's number mod m*, J. Number Theory 128 (2008), 2582-2590.
- [2] J. Bourgain, *Estimates on exponential sums related to the Diffie-Hellman distributions*, Geom. Funct. Anal. 15 (2005) 1-34.
- [3] J. Bourgain and M.Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Camb. Phil. Soc. (2008).
- [4] J. Bourgain, A. Glibichuk and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006) 380-398.
- [5] J. Bourgain and S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Math. Acad. Sci. Paris 337 (2003) 75-80.
- [6] J. Cipra, *Waring's number in a finite field*, Integers 9 (2009), A34, 435-440.
- [7] J. Cipra, T. Cochrane and C. Pinner, *Heilbronn's conjecture on Waring's number (mod p)*, J. Number Theory 125 (2007), 289-297.
- [8] T. Cochrane and J. Cipra, *Sum-product estimates applied to Waring's problem over finite fields*, preprint, 2010.
- [9] T. Cochrane and C. Pinner, *Sum-product estimates applied to Waring's problem mod p*, Integers 8 (2008), A46, 18 pp.
- [10] T. Cochrane and C. Pinner, *Explicit bounds on monomial and binomial exponential sums*, Q. J. Math. 62 (2011) 323-349.
- [11] I. Chowla, *On Waring's problem (mod p)*, Proc. Indian Nat. Sci. Acad. Part A 13 (1943) 195-220.
- [12] S. Chowla, H.B. Mann and E.G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim 32 1959 74-80.
- [13] M.M. Dodson, *On Waring's problem in GF[p]*, Acta Arith. 19 (1971) 147-173.
- [14] M.M. Dodson, *On Waring's problem in p-adic fields*, Acta Arith. 22 (1973) 315-327.
- [15] M.M. Dodson and A. Tietäväinen, *A note on Waring's number in GF[p]*, Acta Arith. 30 (1976) 159-167.



- [16] D.R. Heath-Brown and S.V. Konyagin, *New bounds for Gauss sums derived from  $k$ th powers, and for Heilbronn's exponential sum*, Q. J. Math. 51 (2000) 221-235.
- [17] H. Heilbronn, *Lecture Notes on Additive Number Theory mod  $p$* , California Institute of Technology (1964).
- [18] S. Konyagin, *Estimates for Gaussian sums and Waring's problem modulo a prime*, (Russian) Trudy Mat. Inst. Steklov. 198 (1992), 111-124; translation in Proc. Steklov Inst. Math. 1994, (198), 105-117.
- [19] S. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Mathematics, 136. Cambridge University Press, Cambridge, 1999.
- [20] J. Li and D. Wan, *A new sieve for distinct coordinate counting*, Science in China Series A 53 (2010) 2351-2362.
- [21] J. Li and D. Wan, *Counting subsets of finite Abelian groups*, J. Combin. Theory Ser. A 19 (2012) 170-182.
- [22] A.M. Odlyzko and R.P. Stanley, *Enumeration of power sums modulo a prime*, J. Number Theory 10 (1978) 263-272.
- [23] R.P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge University Press, Cambridge, 1997. Winterhof,
- [24] A. Winterhof and C. van de Woestijne, *Exact solutions to Waring's problem for finite fields*, Acta Arith. 141 (2010) 171-190.
- [25] G. Zhu and D. Wan, *An asymptotic formula for counting subset sums over subgroups of finite fields*, Finite Fields and Their Applications 18 (2012) 192-209.

DEPARTMENT OF MATHEMATICS, SHANGHAI JIAO TONG UNIVERSITY, SHANGHAI, P.R. CHINA  
*E-mail address:* lijyou@sjtu.edu.cn